RECORD AND BRIEFS

Supreme Court, U.S.
FILED
SEP 2 - 2017
OFFICE OF THE CLERK

No. 16-402

In the Supreme Court of the United States

TIMOTHY IVORY CARPENTER,
Petitioner,

v.

UNITED STATES OF AMERICA,
Respondent.

ON WRIT OF CERTIORARI TO THE
UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

BRIEF FOR THE STATES OF ALABAMA, ARIZONA, COLORADO, FLORIDA, IDAHO, INDIANA, KANSAS, KENTUCKY, MARYLAND, MICHIGAN, MONTANA, NEBRASKA, NEW HAMPSHIRE, NEW MEXICO, OKLAHOMA, PENNSYLVANIA, SOUTH CAROLINA, TENNESSEE, AND WYOMING AS AMICI CURIAE IN SUPPORT OF RESPONDENT

Office of the Attorney General
PL-01, The Capitol
Tallahassee, Florida 32399
Amit.Agarwal@myfloridalegal.com
(850) 414-3300

PAMELA JO BONDI
Attorney General of Florida

AMIT AGARWAL
Solicitor General
**Counsel of Record*
DENISE M. HARLE
JORDAN E. PRATT
Deputy Solicitors General

Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES iii

INTEREST OF AMICI STATES 1

SUMMARY OF THE ARGUMENT 2

ARGUMENT 7

I. The Government Does Not "Search" a Phone User When a Neutral and Detached Magistrate Orders a Third-Party Phone Company to Disclose Its Own Cell-Tower Records Pursuant to the Privacy-Protecting Provisions of the SCA 7

A. Petitioner may not assert a constitutionally cognizable privacy interest in historical cell-tower records made, kept, and owned by a third-party service provider. 7

B. Fourth Amendment jurisprudence should not encourage the use of new technologies as instrumentalities of crime. 12

C. This Court's third-party doctrine need not be construed to defeat more substantial expectations of privacy not at issue in this case 14

II. The Challenged SCA Orders Were Constitutionally Reasonable. 16

A. The warrant procedure should not be mechanically applied to congressionally-authorized "searches" arising out of the issuance of compulsory process for third-party cell-tower records. 16

B. As real-world examples make clear, Section 2703(d) orders for cell-tower records serve compelling governmental interests, at little or no cost to individual privacy. 19

C. Congress and the state legislatures should be free to craft reasonable legislative solutions to the difficult problems arising out of compulsory disclosure of third-party records. 25

D. Reasonable considerations support the application for longer-term records in cases like this one. 31

III. Section 2703(d) Is Not Unconstitutional in All Its Applications to Cell-Tower Records. 34

CONCLUSION 36

TABLE OF AUTHORITIES

Cases

Couch v. United States,
409 U.S. 322 (1973) 11

Donaldson v. United States,
400 U.S. 517 (1971) 12

In re Application of the United States for Historical Cell Site Data,
724 F.3d 600 (5th Cir. 2013) 10, 26

Kentucky v. King,
131 S. Ct. 1849 (2011) 17

Kyllo v. United States,
533 U.S. 27 (2001) 3, 13

McMann v. Sec. & Exch. Comm'n,
87 F.2d 377 (2d Cir. 1937) 24

Nw. Austin Mun. Utility Dist. No. One v. Holder,
557 U.S. 193 (2009) 20

Okla. Press Pub. Co. v. Walling,
327 U.S. 186 (1946) 5, 18

Rawlings v. Kentucky,
448 U.S. 98 (1980) 8

Riley v. California,
134 S. Ct. 2473 (2014) 25

Sec. & Exch. Comm'n v. Jerry T. O'Brien, Inc.,
467 U.S. 735 (1984) 11

Smith v. Maryland,
442 U.S. 735 (1979) ..... passim

United States v. Carpenter,
819 F.3d 880 (6th Cir. 2016) 13, 19, 32

United States v. Davis,
785 F.3d 498 (11th Cir. 2015) (en banc) ..... passim

United States v. Graham,
846 F. Supp. 2d 384 (D. Md. 2012) 11, 14

United States v. Jones,
565 U.S. 400 (2012) 27, 36

United States v. Karo,
468 U.S. 705 (1984) 18, 36

United States v. Knotts,
460 U.S. 276 (1983) 16, 36

United States v. Miller,
425 U.S. 435 (1976) ..... passim

United States v. Nixon,
418 U.S. 683 (1974) 26

United States v. Oreckinto,
2017 WL 131563 (D. Conn. Jan. 13, 2017) 23

United States v. Oreckinto,
2017 WL 1371255 (D. Conn. Apr. 14, 2017) 23

United States v. Oreckinto,
234 F. Supp. 3d 360 (D. Conn. 2017) 23

United States v. R. Enters.,
498 U.S. 292 (1991) 24

United States v. Warshack,
631 F.3d 266 (6th Cir. 2010) 15

United States v. Watson,
423 U.S. 411 (1976) 19

Wash. State Grange v. Wash. State Republican Party,
552 U.S. 442 (2008) 35

Wyoming v. Houghton,
526 U.S. 295 (1999) 18

Statutes

18 U.S.C. §2702(c) 16

18 U.S.C. §2703(c)(1)(B) 1

18 U.S.C. §2703(d) ..... passim

2014 Md. Laws Ch. 191 28

725 Ill. Comp. Stat. 168/10 30

Cal. Penal Code §1546.1(e) 31

Cal. Penal Code §1546.1(g) 31

Cal. Penal Code. §1546.1(d)(2) 30

Colo. Rev. Stat. §16-3-303.5(1)(d) 28

Conn. Gen. Stat. §54-47aa 31

Conn. Stat. §54-47aa 28

La. Rev. Stat. §844.9B.(4)–(5) 30

Md. Code Ann. Crim. §1-203.1(d) 31

Me. Rev. Stat. tit. 16 §649 31

Minn. Stat. §626A.42 28

Minn. Stat. §626A.42(1)(e) 28

N.H. Rev. Stat. Ann. §644-A 28

N.H. Rev. Stat. Ann. §644-A:61.V 28

R.I. Gen. Laws §12-32-3 31

Utah Code Ann. §77-22-2.5(2) 30

Utah Code Ann. §77-23c-102(1)(a) 30

Utah Code Ann. §77-23c-102(1)(b) 30

Utah Code Ann. §77-23c-102(1)(d) 31

Va. Code Ann. § 19.2-70.3(E) 30

Va. Code Ann. §19.2-70.3(B) 29

Vt. Stat. Ann. tit. 13, §8102(g) 31

Vt. Stat. Ann. tit. 13, §8103 31

Vt. Stat. tit. 12, §8102(f) 16

Other Authorities

En Banc Brief for the United States, *United States v. Davis* (11th Cir. 2014) (No. 12-12928), 2014 WL 7232613 9

Filings of Defendant, United States v. Carpenter, No. 12-cr-20218 (E.D. Mich.) 8, 34

Subpoena, XVII Oxford English Dictionary 50 (2d ed. 1989) 13

Constitutional Provisions

U.S. CONST. amend. IV 7

INTEREST OF *AMICI* STATES

Amici are the States of Alabama, Arizona, Colorado, Florida, Idaho, Indiana, Kansas, Kentucky, Maryland, Michigan, Montana, Nebraska, New Hampshire, New Mexico, Oklahoma, Pennsylvania, South Carolina, Tennessee, and Wyoming.[1]

This case involves a challenge to the constitutionality of a statute authorizing a "governmental entity" to apply for a non-warrant court order compelling third-party telephone-service providers to produce historical cell-tower records that are "relevant and material to an ongoing criminal investigation." *See* 18 U.S.C. §2703(c)(1)(B), (d). State law-enforcement authorities rely heavily on such orders, which may be sought by state prosecutors and issued by state judges, *id.* §§2703(c)(1)(B), (d), 2711(3)(B), (4), and which "are routinely used to investigate the full gamut of state and federal crimes, including child abductions, bombings, kidnappings, murders, robberies, sex offenses, and terrorism-related offenses." *United States v. Davis*, 785 F.3d 498, 518 (11th Cir. 2015) (en banc). Accordingly, *amici* states have a substantial interest in the Court's disposition of this case.

---

[1] No counsel for any party authored this brief, in whole or in part, and no person or entity other than amici contributed monetarily to its preparation or submission. The parties lodged blanket consents with the Clerk.

SUMMARY OF THE ARGUMENT

I. No "search" of which Petitioner has standing to complain took place when two telephone companies produced their own routing-related records to the government.

A. The Fourth Amendment protects "[t]he right of the people to be secure in *their* . . . papers," not in the papers of *others*. Nevertheless, Petitioner asks this Court to hold that he has a constitutionally cognizable privacy interest in business records that he did not make or own and has never seen or kept, and that contain information he voluntarily conveyed to a third party. That claim fails on its own terms, and it cannot be reconciled with the principles enunciated in this Court's prior cases. Indeed, Petitioner's claim is substantially weaker than the claims this Court rejected in *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976).

B. Petitioner's use of a cell phone does not give him a Fourth Amendment right to conceal information that otherwise would not have been private. A cell site is a cell *tower*, not the site of a cell *phone*. The "cell-site" records Petitioner sought to suppress identify the cell towers used to connect incoming and outgoing calls. Before cell phones were in use, such calls had to be routed via landline telephones tied to fixed and readily identifiable locations; and calls using such phones would have generated third-party records revealing much more specific location-related data than the general vicinity information circumstantially discernible from cell-tower records. That was the case in *Smith*, which approved the acquisition of pen-register data tending

to place petitioner inside a constitutionally protected place—his own home. *See* 442 U.S. at 737.

In other words, the Fourth Amendment should not "permit police technology to erode the privacy guaranteed by the Fourth Amendment," *Kyllo v. United States*, 533 U.S. 27, 34 (2001); but it also should not permit private technologies to be used with impunity as instrumentalities of crime—i.e., to conceal information that could not have been shielded from the ordinary truth-seeking tools of the judicial system if older technologies had been used to engage in the same underlying conduct.

C. There is nothing troubling about applying the third-party doctrine to uphold the congressionally regulated and judicially supervised investigative tool at issue here. Under the statutory provision Petitioner asks this Court to strike down, a phone company may not be required to disclose any of its cell-tower data unless and until all three branches of the government acquiesce in the disclosure. That statutory procedure does not *lower* the bar from a warrant to a non-warrant order; it *raises* the bar from an ordinary subpoena to one that incorporates a broad range of additional privacy protections. *Davis*, 785 F.3d at 505–06.

Future cases, which may involve more sensitive data obtained without the safeguards of the Stored Communications Act (SCA), might well raise distinct concerns. Accordingly, this Court should exercise caution in articulating the contours of the third-party doctrine. As the federal Courts of Appeals have recognized, that doctrine need not be construed to defeat

more substantial privacy concerns that are not implicated by compulsory process for the disclosure of cell-tower records under the SCA.

II. Any "search" of Petitioner arguably arising out of a third-party phone company's production to the government of its own records was not "unreasonable" within the meaning of the Fourth Amendment.

A. The Fourth Amendment bars *unreasonable* searches, not *warrantless* searches. The "warrantless" issuance of a court order under §2703(d) does not make that order unreasonable, for three reasons.

1. The SCA goes above and beyond well-established constitutional prerequisites governing the issuance of compulsory process. That settled law does not require the government to get a warrant before a judicial subpoena may issue; and a Section 2703(d) order is, at bottom, a judicial subpoena, albeit one that incorporates additional privacy protections. In any event, the SCA effectuates the "primary purpose" of the warrant procedure—the interposition of a neutral and detached magistrate between law-enforcement officers and the evidence they seek.

2. A traditional Fourth Amendment analysis supports the reasonableness of the challenged court orders. It is no answer to say that the "warrant requirement" already "strikes the appropriate balance" (Pet. Br. 53–54). As applied to compulsory process, this Court's cases hold that requirements "literally applicable in the case of a warrant" are "satisfied" by a *different* reasonableness test. *See Okla. Press Pub. Co. v. Walling*, 327 U.S. 186, 209 (1946). The SCA passes

that test, and Petitioner does not try to argue otherwise. Petitioner may ask this Court to carve out a new exception to that longstanding law; but he should bear the burden of showing that a traditional balancing of interests supports any such doctrinal innovation.

3. A "strong presumption of constitutionality" applies to congressionally-authorized searches. That "strong presumption" should weigh at least as heavily as the ordinary default rule in favor of warrants. And it should apply with particular force to a "search" based on the *Katz* test, since Congress is especially well-positioned to assess contemporary expectations of privacy and to balance those expectations against competing societal interests.

B. As real-world examples illustrate, SCA orders for cell-tower records serve compelling governmental interests—exonerating the innocent, apprehending the guilty, and protecting the public. When obtained pursuant to the privacy-protecting provisions of the SCA, those real-world benefits come at a negligible cost to individual privacy.

C. There is no "simple answer" to the complicated and difficult question of social policy Congress sought to resolve in enacting the SCA. The answer Congress provided—to break up the pertinent investigative power, allocate it among the three branches of government, and require unanimous interbranch cooperation *before* the government may compel a third party to produce any potentially sensitive evidence in its possession—embodies a particularly enlightened and elegant solution. Like the SCA, state legislative enactments protecting location-related information support

the conclusion that the people's elected representatives are up to the task of assessing contemporary expectations of privacy and carefully balancing those expectations against competing societal interests.

D. In cases like this one, reasonable considerations support the application for "longer-term" cell-tower records. Such records help investigators and prosecutors (at the front end) and juries and judges (at the back end) to make sense of the general vicinity information circumstantially discernible from "shorter-term" cell-tower records; and that is the case precisely because, as defendants frequently emphasize, cell-tower records do not disclose the identity or precise location of a phone user. Petitioner is not in a good position to urge otherwise; in the district court, he faulted the government for analyzing *too little*—and not *too much*—cell-tower data. At any rate, it was reasonable for the government to seek four months of cell-tower records when, as here, "specific and articulable facts" established "reasonable grounds to believe" that Petitioner had committed four months of robberies.

III. Assuming *arguendo* that the government violated the Fourth Amendment when it obtained "longer-term" cell-tower records for a phone tied to Petitioner, Section 2703(d) is not unconstitutional in all its applications to cell-tower records. Settled law compels the conclusion that the government may obtain "shorter term" cell-tower data to determine whether a particular phone was in the vicinity of a public crime scene, particularly when such information is obtained from a third party pursuant to a court order authorized by Congress in a privacy-protecting statute.

ARGUMENT

I. THE GOVERNMENT DOES NOT "SEARCH" A PHONE USER WHEN A NEUTRAL AND DETACHED MAGISTRATE ORDERS A THIRD-PARTY PHONE COMPANY TO DISCLOSE ITS OWN CELL-TOWER RECORDS PURSUANT TO THE PRIVACY-PROTECTING PROVISIONS OF THE SCA.

A. Petitioner may not assert a constitutionally cognizable privacy interest in historical cell-tower records made, kept, and owned by a third-party service provider.

The Fourth Amendment protects "[t]he right of the people to be secure in *their* papers," not in the papers of *others*. U.S. CONST. amend. IV (emphasis added). Consistent with the constitutional text, "[t]his Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him [i.e., the third party] to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *United States v. Miller*, 425 U.S. 435, 443 (1976); *see Smith v. Maryland*, 442 U.S. 735 (1979).

The logic of those cases applies here. *See* U.S. Br. 15–36. Indeed, Petitioner's claim is substantially weaker than the claims this Court rejected in *Smith* and *Miller*, for several reasons.

First, and as a threshold matter, Petitioner did not meet his burden of establishing Fourth-Amendment standing to challenge the records he sought to

suppress. *See Rawlings v. Kentucky*, 448 U.S. 98, 104–05 (1980). The records here at issue pertain to a phone registered under the name "Michael Mayers." Pet. App. 76a. In his motion to suppress, Petitioner never acknowledged that the phone in question was his, or that he was using it at the relevant times. *See Filings of Defendant, United States v. Carpenter*, No. 12-cr-20218 (E.D. Mich.), ECF Nos. 196, 214, 216, 223; *Transcript of Jury Trial*, ECF No. 326, at 155–61. To the contrary, he argued (incorrectly) that the government's application for a court order under §2703(d) "provide[d] no connection between the allegations of the investigation and individuals named in the application, Timothy Sanders and Timothy Carpenter." *Id.* ECF No. 223, at 3; No. 326, at 159; *see also id.* ECF No. 333, at 71 (asserting, in closing argument to the jury, that the agent who testified about cell-tower records "really just talked to you about numbers on cell phones and where he saw the calls made," and didn't "have any direct information about Timothy Carpenter").

Those omissions matter. Modern-day criminals frequently obtain disposable burner phones that may be registered under fictitious aliases and used as instrumentalities of crime.[2] That trend significantly

---

[2] In *Davis*, for example, the defendant used a MetroPCS phone "registered to 'Lil Wayne.'" 785 F.3d at 503. That company—the same company whose service Petitioner used—did "not require[] the subscriber . . . to give his true name," and offered pay-as-you-go plans allowing easy cancellation of service. *See id.* at 503 n.5. Davis never admitted that he owned or possessed the phone in question. At trial, defense counsel emphasized that the government's cell-tower expert did not know whether the phone in

hampers law-enforcement investigations. And it makes it all the more important for the courts to enforce traditional rules governing the assertion of Fourth Amendment standing.

In other words, Petitioner had the option of distancing himself from the phone that was registered under the name "Michael Mayers"; and he could also have tried to assert a reasonable expectation of privacy in third-party records pertaining to that phone. But he did not have the right to do both at the same time.

Second, service contracts and privacy policies typically warn cell-phone customers that phone companies collect location-related information and may disclose such data to law-enforcement authorities. *See In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600, 613 (5th Cir. 2013). For example, MetroPCS's current privacy policy, which is accessible from the company's website, advises its wireless customers that the company "may disclose, without your consent, the approximate location of a wireless device to a governmental entity or law enforcement authority when we are served with lawful process." Similarly, the company warns that its "systems capture details about the . . . location of wireless device(s) you use"; that it "use[s] location information

---

question belonged to his client. The expert's cell-tower maps, defense counsel argued, would have indicated that the phone belonged to "Mickey Mouse" if the agent had been "told to do that" by the prosecutor. *See* En Banc Brief for the United States, *United States v. Davis* (11th Cir. 2014) (No. 12-12928), 2014 WL 7232613, at **9–11.

to route wireless communications and to provide 911 service, which allows emergency services to locate your general location"; and that it "allow[s] third parties the capability of accessing data about your location that is derived from our network."[3] *See also Smith*, 442 U.S. at 742–43 (considering publicly available information included in phone books and other sources in assessing whether Smith had an expectation of privacy in pen-register records). Such express warnings and contractual provisions, even if not dispositive, at least undermine Petitioner's assertion that he actually manifested an objectively reasonable expectation of privacy in MetroPCS's routing-related records.

Third, the Court in *Miller* held that a customer did not have a reasonable expectation of privacy in certain records made and kept by his bank, even though the bank was required by law to maintain those records. *See Miller*, 425 U.S. at 436, 441. In contrast, "[f]ederal law does not mandate that cellular providers create or maintain [historical cell tower] data," *United States v. Graham*, 846 F. Supp. 2d 384, 398 & n.11 (D. Md. 2012) (citing 47 C.F.R. 42.6). Hence, Petitioner's claim is "substantially weaker" than the claim the Court rejected in *Miller*. *See Sec. & Exch. Comm'n v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 n.11 (1984).

Arguments to the contrary are not persuasive.

1. Petitioner may not make out a right to be secure in someone else's "papers," *see* U.S. Const. amend. IV,

---

[3] MetroPCS Privacy Policy, *available at:* https://www.metropcs.com/terms-conditions/privacy.html (last visited October 2, 2017).

by asserting that those papers contained "his location data." Evidence lawfully in the possession of a third party is not *his*, even if it has to do with *him*. Indeed, the Fourth Amendment would not shield Petitioner from incriminating information in records turned over by a third party even if they were his. *See, e.g., Couch v. United States*, 409 U.S. 322, 324, 335–36 (1973) (holding that petitioner could not reasonably claim a Fourth Amendment expectation of privacy in records in which she "retained title" after she had "surrendered possession of the records" to her accountant).

2. As Respondent explains, Petitioner voluntarily conveyed the general vicinity information discernible from cell-tower records. U.S. Br. 21, 23–32. Properly understood, however, such voluntary conveyance is a sufficient—not a necessary—condition for the application of the third-party doctrine. For example, Petitioner did nothing to "convey"—and he may not even have known—the phone numbers of accomplices who called him (*see* J.A. 136). Regardless, he had no right to bar a third party from producing such non-privileged evidence to the government in compliance with a court order authorized by statute, even though that record supplies evidence of associations he might prefer to keep private. Similarly, it does not matter whether Petitioner meaningfully consented to the disclosure of the company's cell-tower records. Like the security-surveillance tapes introduced into evidence at his trial, such evidence was not his to withhold. *See Donaldson v. United States*, 400 U.S. 517, 545 (1971) (Douglas, J., concurring) ("There is no right to be free from incrimination by the records or testimony of others.").

3. This case does not involve governmental "surveillance" or "monitoring" of any kind. Under the SCA, law-enforcement officers do not and may not seek historical cell-tower records to spy on citizens or keep track of their comings and goings. Instead, they consult such records to help resolve questions of historical fact "relevant and material to an ongoing criminal investigation," §2703(d)—in this case, for example, whether Petitioner really was, as accomplices testified, close to the sites of various armed robberies at the times in question. For purposes of that inquiry, the phone company stands in the same shoes as any other witness lawfully in possession of non-privileged evidence relevant to an ongoing criminal investigation. The government does not engage in "surveillance" or "monitoring" when a court compels the production of preexisting documentary (or testimonial) evidence from such a witness, just as a grand jury does not "track" a suspect's movements when it issues a subpoena for a third-party business's security-surveillance videos to find out if a suspect was at the scene of a crime.

B. Fourth Amendment jurisprudence should not encourage the use of new technologies as instrumentalities of crime.

1. This case does not involve governmental use of a "new technology," Pet. Br. 15. Rather, the only tool the government used in this case—i.e., compulsory process for the production of preexisting evidence—is older than the Constitution itself. *See* Subpoena, XVII Oxford English Dictionary 50 (2d ed. 1989) ("He woll not come withoute he have a suppena.") (quoting letter

written in 1467). In 1768, for example, William Blackstone explained that books and papers "in the hands of third persons" "can generally be obtained by rule of court, or by adding a clause of requisition to the writ of *subpoena*, which is then called a *subpoena duces tecum*." *Id.* (quoting 1768 edition of the *Commentaries on the Laws of England*; emphases in the Oxford English Dictionary).

2. The use of §2703(d) orders for cell-tower records does not "diminish[] the degree of privacy that individuals reasonably expected prior to the" invention and widespread dissemination of mobile phones (Pet. Br. 10). *See Kyllo*, 533 U.S. at 34. The cell-tower records Petitioner sought to exclude show that a particular phone used certain towers belonging to the phone company "at call origination and at call termination for incoming and outgoing calls." *United States v. Carpenter*, 819 F.3d 880, 884, 886 (6th Cir. 2016). Before cell phones were invented, Petitioner could not have made or received the calls in question without revealing location-related information to a third-party service provider. Instead, Petitioner would have had to use stationary landline telephones tied to fixed locations; and calls using such phones would have generated third-party records revealing much more precise location-related information than the general vicinity information circumstantially discernible from cell-tower records. *See Smith*, 442 U.S. at 737; *Graham*, 846 F. Supp. 2d, at 399.

In other words, Petitioner did not lose anything in the way of preexisting Fourth Amendment rights when he chose to use a cell phone to make and get calls before, during, and after he committed the robberies of

which he was convicted—and while he was still close to the scene of each crime. That is because Petitioner could not have lost what he never had; and he never had a Fourth Amendment right to make or get a call without revealing to a third-party service provider location-related information incidental to the transmission of that communication. *See Smith*, 442 U.S. at 744–45.

C. This Court's third-party doctrine need not be construed to defeat more substantial expectations of privacy not at issue in this case.

There is nothing troubling about applying the third-party doctrine to uphold the congressionally regulated and judicially supervised investigative tool at issue here. Under the statutory procedure the government invoked in this case, a phone company may not be required to disclose any of its own cell-tower data to the government unless and until all three branches of the government acquiesce in the disclosure. *See* §2703(d). Congress must have authorized the issuance of a requested court order; a law-enforcement officer serving in the executive branch must determine that it is proper to invoke that statutory authority in the particular circumstances at hand; and a neutral and detached magistrate serving in the judicial branch must find that the government has adduced "specific and articulable facts" establishing "reasonable grounds to believe" that the requested third-party records are "relevant and material to an ongoing *criminal* investigation," *i.e.*, to an inquiry that implicates particularly compelling interests in exonerating the innocent, apprehending the guilty, and protecting the public. *See* 18

U.S.C. §2703(d) (emphasis added). Under established Fourth Amendment principles, that statutory procedure does not *lower* the bar from a warrant to a §2703(d) order; it *raises* the bar from an ordinary subpoena to one that incorporates a broad range of additional privacy protections. *Davis*, 785 F.3d at 505–06.

Future cases, which could involve more sensitive data obtained without the safeguards of the SCA, may well raise distinct concerns. Accordingly, this Court should exercise caution in articulating the contours of the third-party doctrine. As the federal Courts of Appeals have recognized, that doctrine need not be construed to defeat more substantial privacy concerns that are not implicated by compulsory process for the disclosure of cell-tower records under the SCA. *See, e.g.*, *Davis*, 785 F.3d at 505 (distinguishing cases involving the use a GPS device, a physical trespass, or real-time or prospective location tracking); *United States v. Warshak*, 631 F.3d 266, 282–86 (6th Cir. 2010) (requiring warrant before obtaining contents of email communications from an email service provider).

The "reality" of the investigative tool at issue here "hardly suggests abuse." *See United States v. Knotts*, 460 U.S. 276, 283 (1983). Indeed, the whole point of the SCA is to *prevent*—not to *permit*—"unfettered" acquisition of potentially sensitive third-party information. That is why, to take just one example, the SCA generally prohibits private phone companies from *voluntarily* sharing their own data with "a governmental entity." *See* 18 U.S.C. §2702(c)(4), (6); *see also, e.g.*, Vt. Stat. tit. 12, §8102(f). "As that prohibition underscores, a telephone company (like MetroPCS) would,

absent privacy-protecting laws (like the SCA), be free to disclose its historical cell tower location records to governmental and non-governmental entities alike—without any judicial supervision," "without having to satisfy the statutory standard in §2703(d)," and without even implicating the Fourth Amendment. *Davis*, 785 F.3d at 506.

If and when Congress and the state legislatures seek to authorize, and private companies make possible, "dragnet type law enforcement practices," "there will be time enough then to determine whether different constitutional principles may be applicable." *Knotts*, 460 U.S. at 284. In the meantime, this Court's Fourth Amendment jurisprudence should be adapted to the realities of the world that we live in, not based on hypothetical scenarios that have nothing to do with facts of this case or the eminently reasonable investigative tool Petitioner asks this Court to strike down. *See id.*

II. THE CHALLENGED SCA ORDERS WERE CONSTITUTIONALLY REASONABLE.

A. The warrant procedure should not be mechanically applied to congressionally-authorized "searches" arising out of the issuance of compulsory process for third-party cell-tower records.

The Fourth Amendment bars *unreasonable* searches, not *warrantless* searches. *Kentucky v. King*, 131 S. Ct. 1849, 1858 (2011). Any arguable "search" of Petitioner arising out of a phone company's disclosure to the government of its own routing-related records

was constitutionally reasonable. At least three considerations support that conclusion.

First, the SCA goes "above and beyond" traditional constitutional prerequisites governing the issuance of compulsory process. *Davis*, 785 F.3d at 506 (discussing "privacy-protection provisions" of the SCA). "[T]he Fourth Amendment, *if applicable to subpoenas for the production of business records and papers, at the most* guards against abuse only by way of too much indefiniteness or breadth in the things required to be 'particularly described,' if also the inquiry is one the demanding agency is authorized by law to make and the materials specified are relevant." *Miller*, 425 U.S. at 445–46 (emphasis added; quotation marks and brackets omitted).

It is not a problem that the SCA omits some of the protections ordinarily tied to the warrant procedure, such as the probable-cause standard and the requirement that facts be attested under oath. As applied to compulsory process, "[t]he requirement of 'probable cause, supported by oath or affirmation' literally applicable in the case of a warrant is satisfied, in that of an order for production, by the court's determination that the investigation is authorized by Congress, is for a purpose Congress can order, and the documents sought are relevant to the inquiry." *Walling*, 327 U.S. at 209. Petitioner's complaints concerning the SCA's departures from the warrant procedure ring particularly hollow in light of the warrant-like protection afforded by the statute. After all, "[t]he primary reason for the warrant requirement is to interpose a 'neutral and detached magistrate' between the citizen

and the 'officer engaged in the often competitive enterprise of ferreting out crime,'" *United States v. Karo*, 468 U.S. 705, 717 (1984), and the SCA does just that.

In short, the challenged court orders comply with applicable Fourth Amendment requirements. Hence, those orders are constitutionally reasonable, even if Petitioner has "the requisite Fourth Amendment interest to challenge the validity" of those orders. *Miller*, 425 U.S. at 446; *see also Walling*, 327 U.S. at 208.

Second, a traditional Fourth Amendment analysis independently supports the reasonableness of the challenged court orders. *See Wyoming v. Houghton*, 526 U.S. 295, 300 (1999). Petitioner "had at most a diminished expectation of privacy in business records made, kept, and owned by [a third-party service provider]; the production of those records did not entail a serious invasion of any such privacy interest, particularly in light of the privacy-protecting provisions of the SCA; [and] the disclosure of such records pursuant to a court order authorized by Congress served substantial governmental interests." *Davis*, 785 F.3d at 518.

Third, there is a "strong presumption of constitutionality due to an Act of Congress, especially when [a constitutional challenge] turns on what is 'reasonable'" within the meaning of the Fourth Amendment. *United States v. Watson*, 423 U.S. 411, 416 (1976). That "strong presumption" should weigh at least as heavily as the general default rule against warrantless searches. Indeed, deference to Congress is particularly appropriate when, as here, any arguable "search" is based on the amorphous "*Katz* standard," which asks

whether an "asserted expectation of privacy is one that *society* is prepared to recognize as reasonable.'" *Carpenter*, 819 F.3d at 889–90 (emphasis added; quotation marks omitted). In that context, "one might say that society itself—in the form of its elected representatives in Congress—has already struck a balance that it thinks reasonable." *Id.* at 890.

Petitioner is wrong to suggest that this case does not involve a congressionally-authorized production. The cell-tower records Petitioner sought to suppress were produced pursuant to a court order issued under 18 U.S.C. §2703(d). Pet. App. 36a. And Petitioner has not asked this Court to review the district court's ruling that the challenged court orders were authorized by statute. *See* Pet i; Pet. App. 39a-40a. Hence, the issue in this case is whether the SCA is unconstitutional insofar as it authorized the government to obtain the historical cell-tower records in question. *See* Pet. App. 36a. That issue implicates the "gravest and most delicate duty" this Court is called on to perform, *see Nw. Austin Mun. Utility Dist. No. One v. Holder*, 557 U.S. 193, 204 (2009) (quotation marks omitted), and calls for the full measure of deference to which congressional enactments are entitled.

B. As real-world examples make clear, Section 2703(d) orders for cell-tower records serve compelling governmental interests, at little or no cost to individual privacy.

"[L]ike other forms of compulsory process not subject to the warrant procedure," §2703(d) orders for cell-tower records are "particularly valuable during the early stages of an investigation," when they "help to

build probable cause against the guilty, deflect suspicion from the innocent, aid in the search for truth, and judiciously allocate scarce investigative resources." *Davis*, 785 F.3d at 518. Real-world examples help to show why that is so, and how such orders are used during the course of day-to-day law-enforcement investigations.

1. In 2011, law-enforcement authorities investigated a series of seven armored-car robberies in Atlanta, Georgia. During one of the robberies, one security guard was murdered and another suffered serious injuries resulting from multiple gunshot wounds. After identifying one of the possible suspects, the FBI obtained call-detail records reciting the phone numbers of people with whom the suspect had been communicating within an hour of each robbery. Investigators lacked probable cause to believe that those other people had committed a crime; but they reasonably suspected that the subject may have been communicating with confederates just before and after the robberies were committed. Accordingly, they obtained §2703(d) orders for approximately 20 people with whom the subject had been in contact during the times in question. Based on those records, the FBI preliminarily excluded 15 potential suspects and identified five additional suspects who were near the robberies and warranted additional investigation. The five additional suspects, along with the initial suspect, all pleaded guilty. (Source: FBI/CAST. N.D. Ga. Case No. 1:11-CR-255.)

2. In 2014, the so-called "Bulls Bandit" robbed two banks in California over a two-month period. Both times, the robber obtained cash from bank tellers after

threatening to detonate a bomb. The robber bore at least some resemblance to a parolee already known to law-enforcement authorities, but the FBI was not able to positively identify that parolee as the robber. Historical cell-tower records obtained under §2703(d) showed that the parolee's phone had communicated with towers near both of the victim banks around the times of the robberies. Based on that information as well as the physical resemblance, the FBI developed probable cause supporting a search warrant, which turned up evidence of the robberies. (Source: U.S. Attorney's Office for the Central District of California. *United States v. Jeremiah Edmond Colino*, Case No. 14-CR-359-PA.)

3. The Phoenix Serial Street Shooter case involved a series of nine shootings, linked together by forensic ballistics evidence, in which seven people were killed. During the investigation, law-enforcement authorities received multiple tips from various members of the public who chose not to identify themselves, presumably out of concern for their own safety. Agents also developed certain investigative leads based on purely circumstantial evidence, such as vehicle descriptions that matched the suspected vehicles, documents showing ownership of the suspected make and model of handguns used, review of social media postings, and previously filed police reports. Due to the anonymous nature of tips received from the general public, and the circumstantial nature of other evidence, agents likely lacked probable cause to believe that any particular suspect committed the shootings.

Cell-tower records obtained under §2703(d) were used to exclude at least two potential suspects. Another suspect could not be included or excluded using those

records; but law-enforcement officers focused other investigative resources on that suspect, which yielded additional physical and circumstantial evidence establishing probable cause to support an arrest. Subsequent investigation linked three additional shootings, resulting in two additional homicides, to the alleged shooter. (Source: FBI/CAST. Maricopa County Superior Court, *Arizona vs. Aaron Juan Saucedo*, Nos. CR2017002335 and CR2017118158.)

4. In March 2011, a warehouse in Wethersfield, Connecticut, was burglarized, and nearly $500,000 worth of cigarettes were stolen. The thief wore a mask, and he also disabled all but one of the surveillance cameras surrounding the warehouse. Twice during the burglary, he was caught on video while holding a cell phone to his ear. The two apparent calls were about an hour apart. With no other leads to go on, law-enforcement agents obtained cell-tower records from the major cell service providers in the area for those two narrow time frames. One number bearing an out-of-state area code showed up with outgoing calls around both time stamps matching the video footage; but it was a burner phone with no identifiable account holder. *See United States v. Oreckinto*, 2017 WL 131563, at *2 (D. Conn. Jan. 13, 2017). Agents then obtained additional call-detail records for that number and began focusing on frequently dialed numbers from the cell phone in question. One frequently dialed number was a family member of a man named Andrew Oreckinto. Agents used that information to find Oreckinto's spouse's Facebook page, which showed a photograph of Oreckinto wearing the same sweatshirt worn by the thief on the warehouse surveillance video. *See United States v. Oreckinto*, 234 F. Supp. 3d 360, 362–64 (D. Conn. 2017)

(denying Oreckinto's motion to exclude images of the sweatshirt).

Using cell-tower records, investigators also linked Oreckinto to three similar burglaries in Connecticut and Pennsylvania in 2009 and 2010. The same burner cell phone number was in the area of two of the burglaries at the time they were committed. A federal jury found Oreckinto guilty of theft of goods from an interstate shipment, in violation of 18 U.S.C. §659, and he also confessed to a 2008 copper theft in New Jersey. *See United States v. Oreckinto*, 2017 WL 1371255 (D. Conn. Apr. 14, 2017). (Source: U.S. Attorney's Office, District of Connecticut.)

Those examples help to illustrate several important points:

First, like other forms of compulsory process not subject to the warrant procedure, historical cell-tower records are an indispensable building block of probable cause. If law-enforcement officers must have probable cause to get such records in the first place, many crimes will never be solved. *See United States v. R. Enters.*, 498 U.S. 292, 297 (1991); *McMann v. Sec. & Exch. Comm'n*, 87 F.2d 377, 379 (2d Cir. 1937) (Hand, J.). And there will be many other cases in which probable cause is developed but comes too late—too late to prevent additional crimes against victims, too late to catch a suspect who has fled, or too late because of the intervening loss or deterioration of other relevant evidence.

Second, §2703(d) orders for cell-tower records frequently help to exonerate the innocent. *See Davis*,

785 F.3d at 518. In some cases, such records are sufficient to exclude potential suspects, and thus spare innocent parties from the substantial burdens of being subjected to a protracted criminal investigation. In others, they at least "deflect suspicion from the innocent," allowing agents to "judiciously allocate scarce investigative resources" by focusing on suspects more likely to be guilty. *See id.*

Third, §2703(d) orders, like other forms of compulsory process, complement rather than displace the warrant procedure. Combined with other evidence, law-enforcement officers routinely use records obtained via compulsory process to obtain probable-cause warrants authorizing more substantial invasions of individual privacy—like the physically disruptive search of a home, a wiretap intercepting the contents of a communication, or a tracking warrant allowing law-enforcement officers to determine the precise location of a telephone (and not just the general vicinity information circumstantially discernible from cell-tower records).

On the other hand, there is no evidence that SCA orders for cell-tower records have ever been abused to the detriment of legitimate privacy interests. In theory, it is possible that rogue law-enforcement officers could obtain such records for legitimate reasons, and then seek to mine them for personal information unrelated to an ongoing criminal investigation. But that same risk is present even if such records are disclosed—as Petitioner concedes is permissible—pursuant to a warrant based on probable cause. In addition, Petitioner does not point to any real-world example in which law-

enforcement authorities used cell-tower records to obtain sensitive information that was not "relevant and material to an ongoing criminal investigation," §2703(d). Nor does he point to any example in which such information was improperly shared in contravention of the statutory bar against improper disclosures. *See* 18 U.S.C. §2707(g). If any such abuse takes place, the SCA "provides remedies and penalties for violations of the Act's privacy-protecting provisions, including money damages and the mandatory commencement of disciplinary proceedings against offending federal officers." *Davis*, 785 F.3d at 506 (citing 18 U.S.C. §§ 2707(a), (c), (d), 2712(a), (c)).

C. Congress and the state legislatures should be free to craft reasonable legislative solutions to the difficult problems arising out of compulsory disclosure of third-party records.

As Petitioner sees it, "this Court should provide a 'simple' answer to the question presented: 'get a warrant.'" Pet. Br. 57–58 (quoting *Riley v. California*, 134 S. Ct. 2473, 2495 (2014)). No matter how this case comes out, the Court should decline Petitioner's invitation to reflexively and mechanically apply the warrant procedure to congressionally authorized searches deemed to arise out of the issuance of compulsory process for third-party business records.

As Congress and the state legislatures have recognized, judicial process for the production of third-party evidence implicates two competing interests, both of which are important. On the one hand, there is a societal interest in protecting the confidentiality of

customer-related information that is exposed to and captured by third-party service providers during the ordinary course of business. *See In re Application for Historical Cell Site Data*, 724 F.3d at 615. On the other hand, there is also a competing societal interest in allowing the government to use ordinary truth-seeking tools to compel the production of non-privileged evidence that is "relevant and material to an ongoing criminal investigation," §2703(d). *See United States v. Nixon*, 418 U.S. 683, 707–09 (1974). Such evidence, after all, is needed to exonerate the innocent and apprehend the guilty; and to do so sooner rather than later, before an innocent person is subjected to a protracted criminal investigation or wrongful incarceration, and before additional crimes are committed against innocent victims, who also—and no less than criminal suspects—have dignity and privacy rights that are deserving of protection. *See* Pet. App. 40a (noting that application recited evidence from a cooperating defendant that the suspects "planned to do additional robberies" and represented that "the cell site records are needed to assist in identifying and locating other persons involved in the robberies").

How should those competing societal interests be balanced? There is no one answer, much less a "'simple' answer," Pet. Br. 58, to that question. The better answer is: *It depends*—on the sensitivity of the information in question, the strength of the relevant societal expectation of privacy, how such evidence is obtained, how much such evidence helps to promote the ends of justice, whether statutory privacy protections accommodate legitimate confidentiality and dignity interests, and a myriad of other factors. All of those factors may change over time, and reasonable people

can disagree about how they should be balanced. *See United States v. Jones*, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring).

The approach Congress took in the SCA—breaking up the pertinent investigative power, allocating it among the three branches of government, and requiring unanimous interbranch cooperation *before* the government may compel a third party to produce any potentially sensitive evidence in its possession—embodies a particularly enlightened and elegant solution. This Court should defer to that eminently reasonable legislative scheme—not because the underlying question of public policy is easy, but because it is hard.

Petitioner's contrary approach would impose a rigid, permanent, one-size-fits-all solution on every state in the country. Such an approach is both unnecessary and unwise.

Congress and the state legislatures are fully capable of protecting sensitive location information. A number of states have enacted statutes specifically regulating the acquisition of location-related information. *E.g.*, Colo. Rev. Stat. §16-3-303.5(1)(d); Minn. Stat. §626A.42(1)(e); N.H. Rev. Stat. Ann. §644-A:61.V. Legislation addressing location data been increasingly common in recent years. *E.g.*, Conn. Stat. §54-47aa(a)(6), (b) (amendment effective October 1, 2017); 2014 Md. Laws Ch. 191 (enacting Md. Code Crim. P. §1-203.1); Minn. Stat. §626A.42 (2014) (new statute governing "Electronic Device Location Information"); N.H. Rev. Stat. Ann. §644-A (2015) (same).

States have adopted a variety of standards for obtaining location-related information. Those standards build on the protections of the SCA, affording greater protections that may stop short of requiring a full-blown warrant. For example, Connecticut law authorizes a judge to compel disclosure of certain "geolocation data" "if the judge makes a finding of probable cause to believe that a crime has been or is being committed and the . . . geolocation data . . . is relevant and material to an ongoing criminal investigation." Conn. Stat. §54-47aa(a)(5), (b) (amendment effective October 1, 2017). That law would seem to provide greater protection than §2703(d) inasmuch as it requires probable cause to believe that *a crime has been committed*. Like §2703(d), however, Connecticut's law does not appear to require probable cause to believe that *the owner or user of the phone has committed a crime* or that incriminating (as opposed to "relevant and material") evidence *will be found in the requested phone records*. *See id.* As Connecticut's solution suggests, reasonable people may disagree about *what* probable cause should look like as applied to the issuance of compulsory process, and not just *whether* probable cause should be required.

Other states have also built on but departed from the standard Congress enacted in §2703(d). Virginia, for example, authorizes a court to order a provider of an electronic communication service to disclose non-content records, excluding real-time location data, "if the investigative or law-enforcement officer shows that there is reason to believe the records or other information sought are relevant and material to an ongoing criminal investigation, *or* the investigation

of any missing child as defined in §52-32, missing senior adult as defined in §52-34.4, or an incapacitated person as defined in §64.2-2000 who meets the definition of a missing senior adult except for the age requirement." Va. Code Ann. §19.2-70.3(B) (emphasis added). As the text after the italicized "or" makes clear, Virginia lawmakers have found that weighty societal interests other than exonerating the innocent and apprehending the guilty—e.g., finding a "missing child" or other vulnerable member of society—may support compulsory disclosure of third-party records.

Legislatures have distinguished between different kinds of "location information," concluding that some deserve more protection than others. For example, it is not uncommon for states to provide greater protections when the government seeks to track an individual by obtaining real-time location information (as opposed to the historical records at issue here). Illinois law provides that "a law enforcement agency shall not obtain current or future location information . . . without first obtaining a court order . . . based on probable cause to believe that the person whose location information is sought has committed, is committing, or is about to commit a crime," or in certain other statutorily specified circumstances. 725 Ill. Comp. Stat. 168/10; *see* Va. Code Ann. § 19.2-70.3(E) (providing that "an investigative or law-enforcement officer may obtain real-time location data without a warrant" only in certain limited circumstances).

As some state laws reflect, the standard by which law-enforcement authorities may obtain third-party records may turn in part on the legislature's assessment of how important it is to investigate a

particular kind of crime. Utah law, for example, generally provides that "a government entity may not obtain" certain "stored data, or transmitted data of an electronic device without a search warrant issued by a court upon probable cause." Utah Code Ann. §77-23c-102(1)(a). But the statute contains an exception authorizing a "prosecutor" to "obtain a judicial order" for certain non-location stored data "[w]hen a law enforcement agency is investigating a sexual offense against a minor, an offense of stalking . . . , or an offense of child kidnapping . . . , and has reasonable suspicion" that a certain kind of communication service "has been used in the commission of a criminal offense." *See id.* §77-22-2.5(2); §77-23c-102(1)(a), (2). If those criteria are satisfied, the law provides that a "law enforcement agent shall" follow procedures akin to—and expressly referencing—"18 U.S.C. § 2703." *Id.* §77-22-2.5(2)(a), (b), (c).

Like Congress, the state legislatures have enacted a broad range of measures to ensure that third-party records are used and handled properly. For example, some states regulate what law-enforcement officers may do with location-related information obtained from a third-party service provider, *e.g.*, Cal. Penal Code. §1546.1(d)(2); La. Rev. Stat. §844.9B.(4)–(5); Utah Code Ann. §77-23c-102(1)(b); require or provide for records to be destroyed within a certain period of time, subject to certain qualifications, *e.g.*, Cal. Penal Code §§1546.1(e)(2), (g); Utah Code Ann. §77-23c-102(1)(d); Vt. Stat. Ann. tit. 13, §8102(g); and mandate that notice be provided to ensure that affected parties are informed in a manner that does not unduly compromise an ongoing investigation, *e.g.*, Conn. Gen. Stat. §54-47aa(f); Md. Code Ann. Crim. §1-203.1(d); Me. Rev.

Stat. tit. 16 §649; R.I. Gen. Laws §12-32-3; Vt. Stat. Ann. tit. 13, §8103.

In short, Congress and the state legislatures are up to the task of protecting legitimate confidentiality interests implicated by compulsory process for third-party business records revealing location-related information. The "simple answer" Petitioner favors—importing, for the very first time, the warrant requirement into the well-established legal regime governing the issuance of compulsory process for third-party records—threatens to cast a cloud of doubt over any number of valuable federal and state laws, to upend centuries of practice, and to preempt ongoing efforts to craft legislative solutions that strike a sensible balance between critical law-enforcement needs and competing confidentiality interests.

D. Reasonable considerations support the application for longer-term records in cases like this one.

The four-month time span of the records at issue here does not make the challenged court orders unreasonable.

Petitioner has not challenged the lower court's ruling that the SCA authorized the issuance of a court order compelling the production of the records at issue here. *See* Pet. i; Pet. App. 39a-40a. Thus, it is undisputed that a federal magistrate judge properly found that the government had adduced "specific and articulable facts" establishing "reasonable grounds to believe" that the requested records were "relevant and material to an ongoing criminal investigation," §2703(d).

In cases like this one, there are good reasons for seeking "longer-term" records of the kind at issue here.

First, longer-term records help investigators to ascertain the identity of the phone user. As noted above, modern criminals frequently obtain disposable burner phones registered under a fictitious alias. And, even when they do not, a mobile phone may regularly be used by someone not listed as the official subscriber. Longer-term cell-tower data help to test allegations or hypotheses that a particular phone belonged to a particular person, by showing whether that phone—even when it was not being used to perpetrate a crime under investigation—was in an area to which that person could be tied by other evidence.

Second, longer-term records help to make sense of the general vicinity information circumstantially discernible from cell-tower records. In rural areas, "a tower's coverage might reach as far as 20 miles." *Carpenter*, 819 F.3d at 885. In urban areas, "each cell site covers 'typically anywhere from a half-mile to two miles.'" *Id.* In either case, cell-tower records show only that a phone was "in the general area" of the place where a crime took place. Pet. App. 45a. Accordingly, short-term cell-tower records have the potential to be misleading. After all, and as defense attorneys frequently argue to juries, a suspect may have had an entirely innocent reason for being in the area in question; for example, he may have lived or worked in that area, or may have been visiting friends or family members.

Longer-term records help to assess those possibilities. Suppose, for example, that a phone was in the

vicinity of a crime scene only once over a two-month period—right around the time when the crime was committed. Such evidence would allow investigators and prosecutors to rule out, and would help juries to assess, the possibility that a suspect just happened to live or work in that area. Similarly, suppose that a phone tied to a suspect was near the scene of many different crimes committed at different times in different locations served by different towers. Such evidence would tend to refute allegations that a suspect just happened to be visiting the neighborhood where any particular crime took place at the time in question. Finally, suppose that a suspect was frequently in the vicinity of the spot where an isolated crime occurred. Such evidence might well support a jury's decision to discount short-term cell-tower data otherwise tending to corroborate the inculpatory testimony of an accomplice.

In short, "longer-term" cell-tower records help investigators and prosecutors (at the front end) and juries and judges (at the back end) to make sense of cell-tower records of the kind at issue here; and that is the case precisely because "shorter-term" cell-tower records, standing alone, cannot be used to conclusively determine the identity or precise location of a phone user.

Petitioner is not in a good position to argue otherwise. Like many modern-day criminals, Petitioner used a phone that was registered under a different name. Pet. App. 76a. And, like many criminal defendants seeking to suppress inculpatory cell-tower records, Petitioner did not admit that the phone in question was his. *See supra* at 8. Although confederates

implicated Petitioner in the charged offenses and testified that the phone in question was his, Petitioner argued that such testimony was unreliable because the robbers were facing "enormous pressure" to lie. *Filings of Defendant, United States v. Carpenter*, No. 12-cr-20218 (E.D. Mich.), ECF No. 333, at 62. And, as is often the case when the prosecution introduces cell-tower evidence, Petitioner's argument to the jury was that the government had erred by analyzing *too little*—and *not too much*—cell-tower data. In closing argument, for example, counsel for Petitioner faulted the government's expert witness because he "didn't put in . . . other records of cell phone calls" on the days in question. *Id.* at 78–79. The agent, defense counsel charged, "wasn't interested in" whether the records, taken as a whole, supported the prosecution's theory, so he included cell-tower data when it supported that theory, but "left it out" when pertinent evidence "didn't fit his theory." *Id.* at 79.

The "longer-term" cell-tower records Petitioner sought to suppress were assuredly "relevant and material" to that defense. Indeed, the government was duty-bound to carefully consider such evidence on its own, before it relied on "shorter-term" cell-tower records as a large part of its case for depriving Petitioner of his liberty.

III. Section 2703(d) Is Not Unconstitutional in All Its Applications to Cell-Tower Records.

Assuming *arguendo* that Section 2703(d) is unconstitutional as applied to "the acquisition of longer-term cell site location information," Pet. Br. 14, this

Court should leave the statute intact as applied to the acquisition of shorter-term cell-tower location data. Petitioner concedes that there is at least "some period of time" over which cell-tower records may be obtained without implicating the Fourth Amendment, *id.* at 30 (quotation marks omitted). And it is a "fundamental principle of judicial restraint" that "courts should neither anticipate a question of constitutional law in advance of the necessity of deciding it nor formulate a rule of constitutional law broader than is required by the precise facts to which it is to be applied." *Wash. State Grange v. Wash. State Republican Party*, 552 U.S. 442, 450 (2008) (quotation marks omitted).

On the merits, there is no viable basis for holding that third-party cell-tower data is always within the phone user's reasonable expectation of privacy—no matter whether the information in question pertains to a single phone call spanning a few seconds or thousands of phone calls spanning a few years, no matter whether the subscriber makes a call in plain view in a public place or from the privacy of his own home, and no matter how explicit the warning incorporated into the customer's service contract. Indeed, such a holding cannot be reconciled with established Fourth Amendment principles.

For example, it is settled law that the police may monitor the whereabouts of suspects traveling in public areas over relatively short periods of time with the aid of electronic devices *surreptitiously* installed in items those suspects obtained from third parties—even if such real-time surveillance is conducted without any judicial supervision or legislative authorization. *See Karo*, 468 U.S. at 707, 712–14); *Knotts*, 460 U.S. at

281–85. In *Jones*, all nine members of this Court stood by that prior precedent. *See* 464 U.S. at 410 ("Karo accepted the container as it came to him, beeper and all, and was therefore not entitled to object to the beeper's presence, even though it was used to monitor the container's location" without his knowledge); *id.* at 430 (Alito, J., concurring in the judgment) (citing *Knotts*, 460 U.S. at 281–82, for the proposition that "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable"). *A fortiori*, investigative agents should be able to obtain the same kind of location information from cell-phone-related technologies of which phone users are expressly and unambiguously warned, particularly when that information is obtained from a third party pursuant to a court order authorized by Congress in a privacy-protecting statute.

CONCLUSION

The judgment of the Court of Appeals should be affirmed.

Respectfully submitted,

PAMELA JO BONDI
Attorney General of Florida

AMIT AGARWAL
Solicitor General
**Counsel of Record*
DENISE M. HARLE
JORDAN E. PRATT
Deputy Solicitors General

Office of the Attorney General
PL-01, The Capitol
Tallahassee, Florida 32399
Amit.Agarwal@myfloridalegal.com
(850) 414-3300

STEVE MARSHALL
Attorney General of Alabama

MARK BRNOVICH
Attorney General of Arizona

CYNTHIA H. COFFMAN
Attorney General of Colorado

LAWRENCE G. WASDEN
Attorney General of Idaho

CURTIS T. HILL, JR.
Attorney General of Indiana

DEREK SCHMIDT
Attorney General of Kansas

ANDY BESHEAR
Attorney General of Kentucky

BRIAN E. FROSH
Attorney General of Maryland

BILL SCHUETTE
Attorney General of Michigan

TIMOTHY C. FOX
Attorney General of Montana

DOUG PETERSON
Attorney General of Nebraska

GORDON J. MACDONALD
Attorney General of New Hampshire

HECTOR H. BALDERAS
Attorney General of New Mexico

MIKE HUNTER
Attorney General of Oklahoma

JOSH SHAPIRO
Attorney General of Pennsylvania

ALAN WILSON
Attorney General of South Carolina

HERBERT H. SLATERY III
Attorney General and Reporter
of Tennessee

PETER K. MICHAEL
Attorney General of Wyoming

October 2, 2017